

CLAIMS

1. A method for modifying an optical path of an optical medium, the optical medium including a first layer adjacent a data layer comprising: selecting a region of the first layer to be distorted; and distorting the region of the first layer such that a reading operation of data stored in the first layer corresponding to the distorted region is modified.
2. The method of claim 1 wherein the first layer comprises the reading layer through which the optical path is directed.
3. The method of claim 1 wherein the optical medium further comprises a back layer adjacent the data layer, opposite the reading layer.
4. The method of claim 1 wherein selecting a region and distorting the region are performed on the reading layer.
5. The method of claim 1 wherein selecting comprises selecting a predetermined region of the first layer.
6. The method of claim 1 wherein selecting comprises selecting a random region of the first layer.
7. The method of claim 1 wherein distortion alters the optical path of the incident light for reading the corresponding data in the data layer.
8. A method for preventing unauthorized use of digital content data stored on a medium comprising: determining one or more data segments in the digital content data, modifying one or more of such data segments to generate modified data comprising second data; storing the modified data at predetermined memory locations on the medium.
9. The method of claim 8 wherein the second data comprises material, such as light sensitive material that is placed to be read as data.

10. The method of claim 8 wherein the digital data comprises data types selected from a group consisting of: audio, video, documents, text or software.
11. The method of claim 8 wherein the data segments are of variable length.
12. The method of claim 8 wherein the second data comprises portions of the digital content data.
13. The method of claim 8 wherein the modified data comprises encrypted data.
14. A method for preventing unauthorized use of digital content data to be transferred from a first system to a second system comprising: locating an archive of a digital content data at the first system; determining transaction data of the second system; determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the archive; and transferring the archive from the first system to the second system if the second system is a valid recipient.
15. The method of claim 14 further comprising if the second system is not a valid recipient after transfer of the archive from the first system to the second system, the operation of the archive failing in the second system.
16. The method of claim 14 wherein the first system may comprise the optical medium or other hard medium, while the second system may comprise a computer on the network or a computer system.
17. The method of claim 14 wherein both the first and second system may comprise computers/computer system.
18. The method of claim 17 wherein the first and second computers/computer systems are remotely located.
19. A method for authenticating a digital medium comprising: monitoring a transfer rate of read-data resulting from the reading of valid data stored on a digital medium at a physical location; determining, from the monitored transfer rate, the presence of an anomaly region on the

digital medium corresponding to the physical location of the valid data on the digital medium; and authenticating the digital medium based on a characteristic of the anomaly region.

20. A system for authenticating a digital medium comprising: a monitor for monitoring a transfer rate of read data resulting from the reading of valid data stored on a digital medium at a physical location; an anomaly detector for determining, from the monitored transfer rate, the presence of an anomaly region on the digital medium corresponding to the physical location of the valid data on the digital medium; and an authenticator for authenticating the digital medium based on a characteristic of the anomaly region.